UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/670,242	09/26/2000	Mark M. Ishikawa		4706

34313 7590 11/05/2008

ORRICK, HERRINGTON & SUTCLIFFE, LLP
IP PROSECUTION DEPARTMENT
4 PARK PLAZA
SUITE 1600
IRVINE, CA 92614-2558

EXAMINER	
LANIER, BENJAMIN E	

ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
11/05/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/670,242	ISHIKAWA ET AL.	
	Examiner	Art Unit	
	BENJAMIN E. LANIER	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 June 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *177-201* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *177-201* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *11/3/2006*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____ .

DETAILED ACTION

Response to Amendment

1. Applicant's amendment filed 11 June 2008 cancels claims 153-176. Claims 177-201 have been added. Applicant's amendment has been fully considered and entered.

Response to Arguments

2. Applicant's arguments with respect to claims have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

5. Claims 177-187 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rabin by U.S. Patent No. 6,697,948, in view of Stratigos, U.S. Patent No. 5,537,486. Referring to claim 177, Rabin discloses an information protection system wherein copyright protection of vendor created software is provided using detection and verification programs. The vendor created

software is distributed with a supervising program that detects whether the software contains an appropriate tag (Col. 20, lines 61-63). If the supervising program discovers that the software is untagged, a fingerprint of the software is computing using selected portions of the software and storing the fingerprint in a fingerprint table of the user device (Col. 20, lines 63-65). A guardian center that includes a fingerprint data structure, and receives all fingerprints from the user devices for each untagged instance of software installed on user devices (Col. 20, line 65 – Col. 21, line 3), which meets the limitation of a data management server system that receives a source file for registration and a target file for comparison with the source file. The fingerprints are generated from selected portions of the software (Col. 20, lines 63-64), which meets the limitation of a key generation system that generates a key for the source file by identifying a predetermined number of source elements in the source file as first source elements. The software vendor identifier can be embedded in the software as a tag (Col. 36, lines 13-16), which meets the limitation of a data embedding system that embeds an information block into the source file, said information block including information pertaining to ownership of intellectual property rights. The fingerprint data structure stored in the guardian center can be stored along with the software in a database (Col. 5, lines 8-10 & Figure 2 element 300), which meets the limitation of a database system that stores the source file with the embedded information block, said key, the first source elements, and ownership information of the source file. A verification program, resident on the guardian center, compares each fingerprint received from the user device against the fingerprints in its fingerprint data structure to determine if an untagged instance of software used on a user device is an infringing instance of software (Col. 21, lines 3-8), which meets the limitation of a source print detection system that compares the first source

elements with corresponding target elements in the target file in accordance with said first unique data identifier and that determines whether coincidence exists between the first source elements in the source file and the target elements in the target file. If the verification program determines that the fingerprints match, punitive action is performed (Col. 58, lines 7-19). One form of punitive action is the notification of the software vendor that created the software (Col. 58, lines 20-23), which meets the limitation of wherein the data management system accesses ownership information to notify an owner of the source file if a first preselected coincidence level exists between the first source elements and the target elements. Rabin discloses that if the supervising program discovers that the software is untagged, a fingerprint of the software is computing using selected portions of the software and storing the fingerprint in a fingerprint table of the user device (Col. 20, lines 63-65). A fingerprint is a unique encoding of one or more portions or data areas selected from an instance of software (Col. 36, lines 52-54). Including a fingerprint of an instance of software within a tag associated with that instance permits a supervising program in a user device to verify that the association between the instance of software and the tag is correct by performing **a same location** fingerprint check on the instance of software and comparing with the list of fingerprints in the associated tag (Col. 36, lines 58-65). This shows that the fingerprints are generating using the same formula or extraction rule, because if you want to compare the fingerprints to determine if instances of software are the same, you would want to extract the same portions of that software for comparison. Otherwise, if you extracted different portions for comparison, the instances of software could be exact copies yet not result in a match upon comparison, which meets the limitation of a source print generation system that applies said first unique data identifier to the source file and extracts the first source elements from the

source file in accordance with said key. Furthermore, this fingerprint would be associated with the extraction rule used in its creation. Otherwise, the supervising program would not know which portions of the instance of software to extract in order to compare the fingerprints as taught in Rabin (Col. 36, lines 61-65). Rabin discloses that the invention is applicable to images (Col. 2, lines 50-53), but does not specify visually inspecting the images when a positive comparison is made. Stratigos discloses a document verification system wherein images of the document are first processed by a computer and then sent to a workstation to be visually examined (Col. 4, lines 12-19), which meets the limitation of visually compared to determine a level of similarity between files. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the suspect and target images of Rabin to be visually examined after being identified as similar in order to provide an additional layer of confirmation as taught by Stratigos (Col. 4, lines 12-19).

Referring to claim 178, Rabin discloses that the fingerprint data structure stored in the guardian center can be stored along with the software in a database (Col. 5, lines 8-10 & Figure 2 element 300), which meets the limitation of said database system is at least partially incorporated with said data management server system.

Referring to claim 179, Rabin discloses that the fingerprints are generated from selected portions of the software (Col. 20, lines 63-64), which meets the limitation of said source print generation system extracts the first source elements being defined by element characteristics selected from the group consisting of an element size, an element start position, and an element initial position relative to said element start position.

Referring to claims 180-181, Rabin discloses that the embedded tags include user-defined information (Col. 36, lines 30-32) and that these tags can be digitally signed (Col. 36, lines 2-4 & Col. 40, lines 43-47), which meets the limitation of said user-defined information is at least partially encrypted.

Referring to claims 182-183, Rabin discloses that the embedded tags can include usage information (Col. 35, lines 14-17), user device id (Col. 36, lines 30-33 & Col. 44, lines 1-8), software identifier (Col. 37, lines 40-45), which meets the limitations of mandatory compliance information, authorized user information, a file description, said mandatory compliance information includes information selected from the group consisting of identification information, custodial information.

Referring to claim 184, Rabin discloses that the guardian server communicates with external computers (Figures 1 & 2), which meets the limitation of said data management system is in communication with at least one external computer system.

Referring to claim 185, Rabin discloses that the tag server and guardian server may be bodily incorporated into the software vendor computer system (Col. 27, lines 48-50), which meets the limitation of the data management system. The software vendor distributes the software to the user's (Figure 2, elements 111 & 112), which meets the limitation of said data management server system provides the source file with said embedded information block to authorize users associated with one or more of the at least one external computer system.

Referring to claim 186, Rabin discloses that the guardian server contains a verification program that communications with a supervising program on the individual user devices to locate target files for comparison against the original source files (Col. 20, line 63 – Col. 21, line

8), which meets the limitation of said source print detection system includes a search member that searches one or more of the at least one external computer system for target files to be compared with the source files.

Referring to claim 187, Rabin discloses an information protection system wherein copyright protection of vendor created software is provided using detection and verification programs. The vendor created software is distributed with a supervising program that detects whether the software contains an appropriate tag (Col. 20, lines 61-63). If the supervising program discovers that the software is untagged, a fingerprint of the software is computing using selected portions of the software and storing the fingerprint in a fingerprint table of the user device (Col. 20, lines 63-65). A guardian center that includes a fingerprint data structure, and receives all fingerprints from the user devices for each untagged instance of software installed on user devices (Col. 20, line 65 – Col. 21, line 3), which meets the limitation of receiving a source file for registration and a target file for comparison with the source file. The fingerprints are generated from selected portions of the software (Col. 20, lines 63-64), which meets the generating a key for the source file by identifying a predetermined number of source elements in the source file as first source elements. The software vendor identifier can be embedded in the software as a tag (Col. 36, lines 13-16), which meets the limitation of embedding an information block into the source file, said information block including information pertaining to ownership of intellectual property rights. The fingerprint data structure stored in the guardian center can be stored along with the software in a database (Col. 5, lines 8-10 & Figure 2 element 300), which meets the limitation of storing the source file with the embedded information block, said key, the first source elements, and ownership information of the source file. A verification program,

resident on the guardian center, compares each fingerprint received from the user device against the fingerprints in its fingerprint data structure to determine if an untagged instance of software used on a user device is an infringing instance of software (Col. 21, lines 3-8), which meets the limitation of comparing the first source elements with corresponding target elements in the target file in accordance with said first unique data identifier and determining whether coincidence exists between the first source elements in the source file and the target elements in the target file. If the verification program determines that the fingerprints match, punitive action is performed (Col. 58, lines 7-19). One form of punitive action is the notification of the software vendor that created the software (Col. 58, lines 20-23), which meets the limitation of accessing ownership information to notify an owner of the source file if a first preselected coincidence level exists between the first source elements and the target elements. Rabin discloses that if the supervising program discovers that the software is untagged, a fingerprint of the software is computing using selected portions of the software and storing the fingerprint in a fingerprint table of the user device (Col. 20, lines 63-65). A fingerprint is a unique encoding of one or more portions or data areas selected from an instance of software (Col. 36, lines 52-54). Including a fingerprint of an instance of software within a tag associated with that instance permits a supervising program in a user device to verify that the association between the instance of software and the tag is correct by performing **a same location** fingerprint check on the instance of software and comparing with the list of fingerprints in the associated tag (Col. 36, lines 58-65). This shows that the fingerprints are generating using the same formula or extraction rule, because if you want to compare the fingerprints to determine if instances of software are the same, you would want to extract the same portions of that software for comparison. Otherwise, if

you extracted different portions for comparison, the instances of software could be exact copies yet not result in a match upon comparison, which meets the limitation of applying said key to the source file, extracting the first source elements from the source file in accordance with said key. Furthermore, this fingerprint would be associated with the extraction rule used in its creation. Otherwise, the supervising program would not know which portions of the instance of software to extract in order to compare the fingerprints as taught in Rabin (Col. 36, lines 61-65). Rabin discloses that the invention is applicable to images (Col. 2, lines 50-53), but does not specify visually inspecting the images when a positive comparison is made. Stratigos discloses a document verification system wherein images of the document are first processed by a computer and then sent to a workstation to be visually examined (Col. 4, lines 12-19), which meets the limitation of visually compared to determine a level of similarity between files. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the suspect and target images of Rabin to be visually examined after being identified as similar in order to provide an additional layer of confirmation as taught by Stratigos (Col. 4, lines 12-19).

Referring to claims 188-189, Rabin discloses that the fingerprints are generated from selected portions of the software (Col. 20, lines 63-64), which meets the limitation of said generating said key includes providing at least one data parameter associated with a selected characteristic of said key and incorporating said at least one data parameter into said key, said source print generation system extracts the first source elements being defined by element characteristics selected from the group consisting of an element size, an element start position, and an element initial position relative to said element start position.

Referring to claim 190, Rabin discloses that the software can contain hashes (Col. 3, line 66 – Col. 4, line 9), which meets the limitation of the source file having data in a compressed format.

Referring to claim 191, Rabin discloses that the fingerprints are generated from the non-hashed information within the software (Col. 20, lines 63-64), which meets the limitation of extracting the source elements includes expanding the data of the source file.

Referring to claim 192, Rabin discloses generating concatenated information from the software (Col. 12, lines 33-39), which meets the limitation of said extracting the source elements includes forming a concatenated string of the source elements.

Referring to claim 193, Rabin discloses that the fingerprinting procedure can be standardized (Col. 4, lines 24-31), which meets the limitation of normalizing data of the source file and extracting the normalized data form the source file.

Referring to claim 194, Rabin discloses that the embedded tags include user-defined information (Col. 36, lines 30-32) and that these tags can be digitally signed (Col. 36, lines 2-4 & Col. 40, lines 43-47), which meets the limitation of partially encrypting said information block.

Referring to claim 195, Rabin discloses that the guardian server communicates with external computers (Figures 1 & 2), which meets the limitation of receiving said source file includes communicating with an external computer system.

Referring to claim 196, Rabin discloses that the guardian server contains a verification program that communications with a supervising program on the individual user devices to locate target files for comparison against the original source files (Col. 20, line 63 – Col. 21, line

8), which meets the limitation of searching one or more of the at least external computer system for target files to be compared with the source file.

Referring to claim 197, Rabin discloses that the tag server and guardian server may be bodily incorporated into the software vendor computer system (Col. 27, lines 48-50), which meets the limitation of the data management system. The software vendor distributes the software to the user's (Figure 2, elements 111 & 112), which meets the limitation of providing the source file with said embedded information block to authorized users associated with one or more of the at least one external computer system.

Referring to claim 198, Rabin discloses that fingerprinting involves a mathematical function for mapping data to smaller data (Col. 30, lines 26-27), which meets the limitation of said extracting the first source elements comprises extracting the first source elements from the source file via compression specific element extraction.

6. Claims 199-201 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rabin, U.S. Patent No. 6,697,948, in view of Stratigos, U.S. Patent No. 5,537,486, and further in view of Agrawal, U.S. Patent No. 5,647,058. Referring to claims 199-201, Rabin discloses that the software can be video data (Col. 2, lines 50-52) and that the fingerprinting involves a mathematical function for mapping data to smaller data (Col. 30, lines 26-27), which meets the limitation of said receiving the source file includes receiving a source file with a plurality data values, said receiving a source file includes receiving a video source file with a plurality of red-green-blue (RGB) data values. Rabin does not disclose fingerprinting the video data by calculating an average value of the RGB data values of portions of the video data. Agrawal discloses a method of indexing a multi-media database wherein video data is fingerprinted using

the average of RGB color features (Col. 6, lines 28-38), which meets the limitations of said extracting the first source elements comprises extracting the first source elements from the source file via non-compression specific extraction, wherein said extracting the first source elements includes calculating an average value of the data values for each of the first source elements, wherein said calculating the average value of the data values comprises calculating an average value of the RGB data values for each of the first source elements. It would have been obvious to one of ordinary skill in the art at the time the invention was made to fingerprint the video data of Rabin using the average of the video RGB data values in order to create indexes for the database that provide similarity characteristics (Agrawal: Col. 2, lines 3-16) such that efficient searching of the database can be achieved as taught by Agrawal (Agrawal Col. 2, lines 38-49).

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to BENJAMIN E. LANIER whose telephone number is (571)272-3805. The examiner can normally be reached on M-Th 7:00am-5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Benjamin E Lanier/
Primary Examiner, Art Unit 2432